IN THE CLAIMS:

Please amend claims 1-20 as follows.

1. (Currently Amended) A system ~~for providing secure mobile connectivity that implements Mobile IP Home Agent functionality via distributed components~~, comprising:

a mobile node belonging to a home network located within a secure network, the mobile node having a network interface configured to communicate with other nodes, the mobile node having only one security association and only one mobility binding with a home agent ~~(HA) for~~so as to provide secure mobile connectivity that implements ~~the~~ a mobile ~~IP~~internet protocol home agent functionality;

a proxy home agent ~~(PHA)~~ connected to the home network and located within the secure network, wherein the ~~PHA~~ proxy home agent is configured to provide a proxying functionality~~,~~;

the ~~HA~~ home agent located outside of the secure network, wherein the ~~HA~~ home agent is configured to provide a signaling and tunneling functionality and to notify the ~~PHA~~ proxy home agent of the mobile node; and

a virtual private network ~~(VPN)~~ gateway located outside the secure network and configured to work in conjunction with the ~~HA~~home agent.

2. (Currently Amended) The system of ~~Claim~~ claim 1, wherein the ~~VPN~~ virtual private network gateway and the ~~HA~~ home agent are located within a single device within a demilitarized zone. ~~(DMZ).~~

3. (Currently Amended) The system of ~~Claim~~ claim 1, further comprising a firewall coupled to the secure network and the ~~VPN~~ virtual private network gateway~~;~~, wherein the ~~HA~~ home agent is located within the firewall.

4. (Currently Amended) The system of ~~Claim~~ claim 1, wherein the ~~HA~~ home agent is a separate device from the ~~VPN~~ virtual private network gateway.

5. (Currently Amended) The system according to claim 1, further comprising:

a demilitarized ~~demilitarised~~ zone ~~(DMZ)~~ located outside the secure network, wherein the virtual private network ~~VPN~~ gateway and the ~~HA~~ home agent reside in the ~~DMZ~~demilitarized zone;

a first firewall between the secure network and the ~~DMZ~~ demilitarized zone; and

a second firewall between the ~~DMZ~~ demilitarized zone and an external network configured to deny communications from the external network with a source address in the known range~~;~~, ~~and~~

wherein the mobile node has a permanent address in a known range.

6. (Currently Amended) The system according to claim 1, further comprising:

a demilitarized ~~demilitarised~~ zone ~~(DMZ)~~ located outside the secure network,

wherein the ~~VPN~~ virtual private network gateway and the home agent reside in the ~~DMZ~~demilitarized zone; and

a first firewall between the secure network and the ~~DMZ~~demilitarized zone~~;~~,

wherein the mobile node has a permanent address in a known range and the first firewall is programmed to deny all communications from the demilitarized zone ~~DMZ~~ with a source address in the known range~~;~~, and

wherein the ~~VPN~~ virtual private network gateway has a direct connection to an internal interface of the first firewall such that the first firewall considers the ~~VPN~~ virtual private network gateway transmitted data as internal to the secure network.

7. (Currently Amended) The system of ~~Claim~~ claim 1, further comprising:

a demilitarized ~~demilitarised~~ zone ~~(DMZ)~~ comprising a first router coupled to a second router that is coupled to a firewall, the ~~VPN~~ virtual protocol network gateway coupled to the first router, and the firewall~~;~~, wherein the ~~HA~~ home agent is coupled to the first router.

8. (Currently Amended) The system of ~~Claim~~ claim 7, wherein packets from the mobile node destined toward nodes inside the secure network first go the ~~HA~~ home

agent and then to the virtual protocol network ~~VPN~~ gateway that is configured to forward the packets through the firewall to the secure network.

9. (Currently Amended) The system of ~~Claim~~ claim 8, wherein packets from the second router to the firewall having a source address in a known range are dropped by the firewall.

10. (Currently Amended) The system according to claim 1, wherein a router is directly connected to a firewall, and the ~~VPN~~ virtual protocol network gateway and the ~~HA~~ home agent are configured to connect to a different interface of the router and the firewall.

11. (Currently Amended) The system of ~~Claim~~ claim 10, wherein the firewall is configured such that it considers the interface with which it connects to the ~~VPN~~virtual protocol network gateway as an internal interface and packets with a source address that are outside of a known address range received on the internal interface are dropped, and packets with a source address that are within the known address range that are received by the firewall on an external interface are dropped.

12. (Currently Amended) The system of ~~Claim~~ claim 11, wherein ~~VPN~~virtual protocol network encapsulated packets are forwarded to the ~~VPN~~ virtual protocol

network gateway and when a security association (~~SA~~) exists, the packet is decrypted and forwarded to the firewall on the internal interface and when a ~~SA~~ security association does not exist the packet is dropped.

13. (Currently Amended) The system of ~~Claim~~ claim 12, wherein mobile ~~IP~~ internet protocol packets and ~~VPN~~virtual protocol network encapsulated packets first reach the home agent which are forwarded to the ~~VPN~~virtual protocol network gateway and then to the secure network through the firewall's internal interface.

14. (Currently Amended) The system of ~~Claim~~ claim 1, further comprising:

a firewall coupled to the secure network and the ~~VPN~~virtual protocol network gateway; and

a router ~~includes~~ comprising an access control list used to drop packets that have a source address that belong to a known address range.

15. (Currently Amended) A method, ~~for secure communication between a mobile node associated with a home network in a secure network and a correspondent node,~~ comprising:

establishing a proxy home agent ~~(PHA)~~ located within the secure network to monitor data directed to the mobile node so as to secure communication between a

mobile node associated with a home network in a secure network and a correspondent node;

establishing a home agent configured to create only one security association with the mobile node and only one mobility binding with the mobile node and to notify the proxy home agent ~~PHA~~ of the mobile node;

collecting data directed to the mobile node;

packaging the collected data in a virtual private network secure tunnel to an internal address of the mobile node to create ~~VPN~~virtual protocol network packaged data; and

tunneling the ~~VPN~~virtual protocol network packaged data to a current address of the mobile node.

16. (Currently Amended) The method of claim 15, wherein the ~~VPN~~virtual protocol network secure tunnel follows the ~~IP~~ internet protocol security protocol.

17. (Currently Amended) The method of claim 15, wherein the tunneling of the ~~VPN~~ virtual protocol network packaged data to the external mobile node occurs according to the ~~IP~~ internet protocol mobility protocol.

18. (Currently Amended) The method of ~~Claim~~ claim 15, further comprising: packaging the collected data in an IP-in-IP tunnel and sending it to a ~~VPN~~virtual protocol

network device for virtual protocol network ~~VPN~~ encryption and tunneling the ~~VPN~~ virtual protocol network packaged data to the current address of the mobile node.

19. (Currently Amended) A system, ~~for secure mobile connectivity that implements mobile IP home agent functionality via distributed components;~~ comprising:

means for establishing a proxy home agent ~~(PHA)~~ located within a secure network to monitor data directed to a mobile node so as to secure mobile connectivity that implements mobile internet protocol home agent functionality via distributed components;

means for establishing a home agent configured to create only one security association with the mobile node and only one mobility binding with the mobile node and to notify the proxy home agent ~~PHA~~ of the mobile node;

means for collecting data directed to the mobile node;

means for packaging the collected data in a virtual private network ~~(VPN)~~ secure tunnel to an internal address of the mobile node to create ~~VPN~~ virtual private network packaged data;

means for tunneling the ~~VPN~~ virtual private network packaged data to a current address of the mobile node;

means for the home agent to communicate to the ~~PHA~~ proxy home agent that the mobile node has moved outside its home network;

means for the home agent to communicate to the ~~PHA~~ proxy home agent that the mobile node has come back to its home network; and

means for enabling the ~~PHA~~ proxy home agent to create and remove a proxy address resolution protocol ~~(ARP)~~ entry for a permanent address associated with the mobile node.

20. (Currently Amended) A computer program embodied on a computer readable medium, the computer program being configured to control a processor to perform:

establishing a proxy home agent ~~(PHA)~~ located within a secure network to monitor data directed to a mobile node;

establishing a home agent configured to create only one security association with the mobile node and only one mobility binding with the mobile node and to notify the ~~PHA~~ proxy home agent of the mobile node;

collecting data directed to the mobile node;

packaging the collected data in a virtual private network ~~(VPN)~~ secure tunnel to an internal address of the mobile node to create ~~VPN~~ virtual private network packaged data; and

tunneling the ~~VPN~~ virtual private network packaged data to a current address of the mobile node.